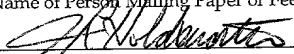
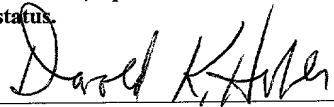
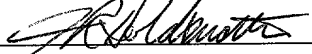


FORM PTO-1390 (REV 10-2000)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY'S DOCKET NUMBER 6400-11WOUS	
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371				U.S. APPLICATION NO. (If known, see 37 CFR 1.5) 09/720353	
INTERNATIONAL APPLICATION NO. PCT/DE00/01086		INTERNATIONAL FILING DATE April 7, 2000		PRIORITY DATE CLAIMED April 30, 1999	
TITLE OF INVENTION SIGNING AND SIGNATURE CHECKING OF MESSAGES					
APPLICANT(S) FOR DO/EO/US Michael Nolte					
<p>Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:</p> <ol style="list-style-type: none"> 1. <input checked="" type="checkbox"/> This is a FIRST submission of items concerning a filing under 35 U.S.C. 371. 2. <input type="checkbox"/> This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371. 3. <input checked="" type="checkbox"/> This is an express request to promptly begin national examination procedures (35 U.S.C. 371(f)). 4. <input checked="" type="checkbox"/> The US has been elected by the expiration of 19 months from the priority date (PCT Article 31). 5. <input checked="" type="checkbox"/> A copy of the International Application as filed (35 U.S.C. 371(c)(2)) <ol style="list-style-type: none"> a. <input type="checkbox"/> is attached hereto (required only if not communicated by the International Bureau). b. <input checked="" type="checkbox"/> has been communicated by the International Bureau. c. <input type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US). 6. <input checked="" type="checkbox"/> An English language translation of the International Application as filed (35 U.S.C. 371(c)(3)). 7. <input checked="" type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19(35 U.S.C. 371(c)(3)) <ol style="list-style-type: none"> a. <input type="checkbox"/> are attached hereto (required only if not communicated by the International Bureau). b. <input type="checkbox"/> have been communicated by the International Bureau. c. <input type="checkbox"/> have not been made; however, the time limit for making such amendments has NOT expired. d. <input checked="" type="checkbox"/> have not been made and will not be made. 8. <input type="checkbox"/> An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)). 9. <input checked="" type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). 10. <input type="checkbox"/> An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)). <p>Items 11 to 16 below concern document(s) or information included:</p> <ol style="list-style-type: none"> 11. <input checked="" type="checkbox"/> An Information Disclosure Statement under 37 CFR 1.97 and 1.98. 12. <input checked="" type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included. 13. <input checked="" type="checkbox"/> A FIRST preliminary amendment. <input type="checkbox"/> A SECOND or SUBSEQUENT preliminary amendment. 14. <input type="checkbox"/> A substitute specification. 15. <input type="checkbox"/> A change of power of attorney and/or address letter. 16. <input checked="" type="checkbox"/> Other items or information: Form PCT/IB/308 					
<div style="text-align: right;"> <p>EXPRESS MAIL™ MAILING LABEL</p> <p>Number <u>EL702049080US</u></p> <p>Date of Deposit <u>December 21, 2000</u></p> <p>I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office To Addressee" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to Box PCT, Commissioner of Patents and Trademarks, Washington, D.C. 20231</p> <p><u>J R Holdsworth</u></p> <p>(Typed Name of Person Mailing Paper or Fee)</p> <p></p> <p>(Signature of Person Mailing Paper or Fee)</p> </div>					

U.S. APPLICATION NO. 09/720353 <small>(if known, see 37 CFR 1.55)</small>		INTERNATIONAL APPLICATION NO. PCT/DE00/01086		ATTORNEY'S DOCKET NUMBER 6400-11WOUS	
17. <input checked="" type="checkbox"/> The following fees are submitted: BASIC NATIONAL FEE (37 CFR 1.492(a)(1)-(5)): Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO \$1000.00 International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO \$860.00 International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO \$710.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) \$690.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) \$100.00 ENTER APPROPRIATE BASIC FEE AMOUNT =				CALCULATIONS PTO USE ONLY 	
Surcharge of \$130.00 for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				\$	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	10 - 20 =	—	X \$18.00	\$	
Independent claims	2 - 3 =	—	X \$80.00	\$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ \$270.00	\$	
TOTAL OF ABOVE CALCULATIONS =				\$ 860.00	
<input type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.				\$	
SUBTOTAL =				\$ 860.00	
Processing fee of \$130.00 for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				\$	
TOTAL NATIONAL FEE =				\$ 860.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property				\$ 40.00	
TOTAL FEES ENCLOSED =				\$ 900.00	
				Amount to be	\$
				refunded:	\$
				charged:	\$
a. <input checked="" type="checkbox"/> A check in the amount of \$ <u>900.00</u> to cover the above fees is enclosed.					
b. <input type="checkbox"/> Please charge my Deposit Account No. <u>13-0235</u> in the amount of \$_____ to cover the above fees. A duplicate copy of this sheet is enclosed.					
c. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. <u>13-0235</u> . A duplicate copy of this sheet is enclosed.					
NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.					
SEND ALL CORRESPONDENCE TO:					
Donald K. Huber McCormick, Paulding & Huber LLP CityPlace II 185 Asylum Street Hartford, CT 06103-3402					
SIGNATURE:  Donald K. Huber Dec. 21, 2000 NAME 18,686 REGISTRATION NUMBER					

"EXPRESS MAIL" MAILING LABEL
NUMBER EL702049080US
DATE OF DEPOSIT December 21, 2000
I HEREBY CERTIFY THAT THIS PAPER OR FEE IS BEING DEPOSITED
WITH THE UNITED STATES POSTAL SERVICE "EXPRESS MAIL POST
OFFICE TO ADDRESSEE" SERVICE UNDER 37 C.F.R. 1.10 ON THE
DATE INDICATED ABOVE AND IS ADDRESSED TO THE
COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON,
D. C. 20231
J. R. Holdsworth
(TYPED NAME OF PERSON MAILING PAPER OR FEE)

(SIGNATURE OF PERSON MAILING PAPER OR FEE)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Application of)
)
for SIGNING AND SIGNATURE CHECKING)
OF MESSAGES)
)
Serial No: National Stage Entry of International) Our Docket No: 6400-11WOUS
Application No. PCT/DE00/01086 filed April 7, 2000)
)
Filed: Simultaneously herewith)

Hartford, Connecticut, December 21, 2000

Box PCT
Assistant Commissioner for Patents
Washington, D. C. 20231

PRELIMINARY AMENDMENT

S I R:

Concurrently with the entry of the above-identified international application into
the U.S. National Stage, please amend it as follows:

In the Specification (of the English Translation of the Application)

Page 1, line 3, delete the sub-heading "Technical field" and substitute --FIELD
OF THE INVENTION--.

Page 1, line 8, delete the sub-heading "Prior art" and substitute --
BACKGROUND OF THE INVENTION--.

Page 2, line 15, delete the sub-heading "Description of the invention" and
substitute --SUMMARY OF THE INVENTION--.

Page 3, lines 13 and 14, delete the sub-heading "Description of at least one embodiment at least of the invention" and substitute --DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS--.

In the Claims (of the English Translation of the Application)

Claim 5 - amend as follows:

5. (Amended) The method as claimed in claim 1, wherein the sequence number is produced by a pseudo-random number generator.

Claim 6 - amend as follows:

6. (Amended) The method as claimed in claim 1, wherein the encryption of the sequence number by means of the main key is used as the one-time encryption.

Claim 7 - amend as follows:

7. (Amended) The method as claimed in claim 1, wherein the control center (10) produces a number of signing keys (14) in advance, and transmits them to the sender (30), possibly together with the associated sequence numbers (12).

Claim 8 - amend as follows:

8. (Amended) The method as claimed in claim 1, wherein the receiver (30) maintains a list of already used sequence numbers, and rejects already used sequence numbers.

Claim 10 - amend as follows:

10. (Amended) The device as claimed in claim 9, wherein a generator using a deterministic method produces one or more sequence numbers corresponding to the number of checks.

In the Abstract

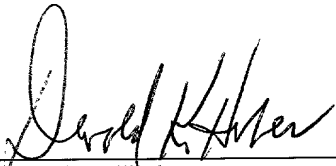
Delete the sub-heading "Abstract" and substitute --Abstract of the Disclosure--;
and on the last line, delete "Figure 1".

REMARKS

The above amendments are requested to put the application into better U.S. format and to delete multiple dependencies.

Any fee required by the filing of this amendment may be charged to our Deposit Account No. 13-0235.

Respectfully submitted,

By 
Donald K. Huber
Registration No. 18,686
Attorney for Applicant

McCormick, Paulding & Huber LLP
CityPlace II
185 Asylum Street
Hartford, Connecticut 06103-4102
(860) 549-5290

09/720353
528 R3c'd PCT/PTO 21 DEC 2000

U. S. National Stage Entry of Int'l. Appln. No. PCT/DE00/01086

Attorney Docket No. 6400-11WOUS

99P6221)

ENGLISH TRANSLATION OF THE APPLICATION

09/720353
528 R3c'd PCT/PTO 21 DEC 2000

Signing and signature checking of messagesTechnical field

- 5 The invention relates to the signing and signature checking of messages using secret keys.

Prior art

- 10 In order to provide protection against corruption of messages, it is known for symmetrical cryptography to be used to form a signature by means of which the receiver can check, with very high probability, whether the message has been transmitted without corruption and
- 15 originates from the predetermined sender. However, one precondition is that the sender and receiver have a common, secret key, which must be stored in secure form. One such method is described, for example, in Patent Specification US 4,549,075.

- 20 Symmetrical cryptography, in particular the DES method, is frequently used in smart cards, because this method can be programmed very efficiently. The smart cards furthermore have a read only memory in which a main key
- 25 is stored in secure and secret form, and this main key is also stored in secure form in a control center.

- If it is now intended to send a message, protected against corruption, from a sender to the receiver, in
- 30 this case the smart card, then, until now, the sender has had to have the message signed by the control center, since the control center cannot provide the sender with the secret main key

without weakening the entire system. Furthermore, measures are required to ensure that the message is protected against corruption and imitation of a legitimate sender during transmission from the sender
5 to the main center.

The object of the invention is thus to specify a method for corruption protection of messages by means of a signature which can be formed by a sender and can be
10 sent to a receiver without the sender having the secret main key, which is shared by the receiver and a control center, or without the message having to be sent in advance to the control center, for signature formation.

15 Description of the invention

The invention uses a method in which the control center forms signing keys in advance, and provides them to the sender. As is described in more detail in the exemplary
20 embodiments, the receiver can model the signing key, and can thus check the message.

This relates to a method for signing a message, in which a control center and the receiver have a
25 permanent, common main key. The control center produces a sequence number in advance, and produces a signing key from this by means of a one-time function. Both are provided to the sender, in secure form. The sender uses the signing key to form a signature for the message,
30 and sends this signature with the sequence number and the message to the receiver. The receiver uses a one-time function, main key and sequence number to form a check key, and thus checks the signature on the message.

Further features and advantages of the invention result from the following description, which explains the invention with reference to an exemplary embodiment and in conjunction with the attached drawing.

5

Brief description of the drawing

In the figures:

- 10 Figure 1 shows a diagram in which the data flow is symbolized, with the components involved.

Description of at least one embodiment at least of the invention

15

Figure 1 indicates the three parties involved in the method, namely the control center 10, the sender 20 and the receiver 30, separated by dashed-dotted lines.

- 20 The control center 10 contains a secure memory 11 for a secret key which is otherwise used, for example, in a symmetrical cryptographic encryption or signing method. The receiver 30 contains a corresponding memory 11', which contains the same key. This key is written to the
25 control center during initialization, for example, if the receiver 30 is a smart card. Otherwise, key distribution methods known from cryptography can be used. In this case, the key is stored only once or at very long time intervals; the storage can be regarded
30 as being permanent for the method according to the invention.

The control center 10 furthermore contains a sequence generator 12. This provides a series of numbers, which each differ. In the simplest case, this is a sequential number. However, it is better to use a known pseudo-random number generator, for example using the modulo method. If the parameters are chosen correctly, these pseudo-random number generators produce a sequence of new numbers in each case until the cycle which is governed by the modulus has been run through. Decreasing numbers or numbers with a step interval greater than unity can also be used. It is likewise possible to use the date and time as a unique sequence number, possibly as the number of seconds since an appointed start.

15 The control center thus produces one or more sequence numbers 12. A one-time encrypter 13 uses the main key to form a signing key 14 from such a sequence number 12. This is most easily done by the sequence number 12 being encrypted by means of the main key. In this case, a short sequence number is filled out by means of further data to the block length of the encryption method. Although binary zeros can be used for this purpose, it is better to use a function of the sequence number, for example its square. It is also possible to use a constant text, which does not consist of binary zeros and is kept confidential. Since the block size is generally in the same order of magnitude as the key length, it is still possible to use the result as a key; if necessary, bits must be added or the number of bits reduced by convolution.

The essential characteristic of the one-time encrypter is that it is virtually impossible to deduce the main

key. Although the method just described is not a one-time encryption since, for example, the receiver could form the sequence number from the signing key by decryption, the "one-time" functionality is the main
5 feature.

Other one-time functions are thus used in other embodiments which link the main key and the sequence number in a reproducible manner to form a signing key
10 without anyone who does not have the main key relating to a given sequence number being able to form a valid signing key, or vice versa, or being able to determine the main key from the signing key and the sequence number. Such methods are generally referred to as
15 "message authentication codes" (MAC). One such method may be formed, in particular, by applying any desired cryptographically secure one-time function to a combination of a main key and sequence number. A concatenation, exclusive-OR, multiplication with or
20 without modulo formation or addition, etc., may be used as the combination.

The control center 10 thus provides one or more pairs of sequence numbers 12, and signing keys 14 produced
25 from them. This can be done, for example, by printing out on security paper, by storage in a further smart card or by some other secure data transmission. These pairs are provided to the sender 20 in advance, who must store them in a secure and confidential manner.

30
The sender 20 who wishes to send a message 21 to the receiver 30 takes a pair of sequence numbers 12 and signing keys 14 and uses the signer 24 to determine the signature for the message 21. The DES method, for
35 example

in accordance with ANSI X9.9, is preferably also used in this case. Alternatively, a signature can be produced by a combination of a cryptographic hash function and a message authentication code. Methods
5 relating to this have been described frequently and comprehensively in the cryptographic literature.

The sender then forms a data set 22, which contains three fields with the sequence number 22a, the message
10 22b and the signature 22c. The signing key 14 which has just been used is deleted.

The data set 22 is now transmitted to the receiver 30, which thus receives a data set 22' which once again
15 contains three fields, which are regarded as the sequence number 22a', the message 22b' and the signature 22c'. Normally, this data set has already been protected against transmission errors by other security or plausibility mechanisms.

20 The receiver extracts the sequence number 22a' from the received data set 22', and passes this together with the main key 11' to one-time encryption 13' which, in the same way as the one-time encryption 13, is located
25 in the control center 10 and is functionally identical to it. A check key 14' is produced at the output of the one-time function. If the sequence number has been transmitted correctly, this check key 14' is identical to the signing key 14 which the sender 20 has used. The
30 check key 14' is passed to a signature checker 38 together with the message 22b' which has arrived and the signature 22c' which has arrived. If all three match one another, an enable signal for further use of the message is produced at the output of the signature
35 checker 38. At the end of the check, the check key 14' is destroyed, irrespective of the result.

In one development of the invention, the receiver maintains a list of already used sequence numbers, and rejects messages with already used sequence numbers. This provides additional security against misuse.

5

Since the sequence number is preferably produced by a deterministic generator, there is no need to transmit the sequence number. Since the common main key has to be transmitted in a secure environment to the receiver
10 in any case, the initial value of the generator can be transmitted at the same time. Whenever a message is received, the receiver produces a new value for the sequence number, and thus forms the check key 14' without the sequence number having to be transmitted as
15 well. In order to be robust against double transmissions and lost messages, one of the last and following sequence numbers is expediently also then used. In this case as well, the control center can provide the sender with a number of signing keys 14,
20 which the sender should then use in the predetermined sequence.

One possible application of the invention is in the field of automatic cash dispensers. The control center
25 is in this case the bank control center, which uses a main key for checking the PIN and supplies personalized checking modules to the manufacturer of automatic cash dispensers in the control center. The sender may be a manufacturer or a local bank organization which, for
30 example, wishes to load a currency conversion rate or a discount rate into the automatic cash dispensers; however, such organizations cannot introduce their own secret key into the cash dispenser, nor do they wish to install their own security module.

If the receiver does not contain a non-volatile memory, the receiver can also produce the sequence numbers from the start and test the signature with each of them. The loss of security in this case is low, but this does not provide any protection against double use.

5

Patent Claims

1. A method for signing a message (22) by a sender (20), and for checking the signature by a receiver (30), wherein a control center (10) and a receiver (30) have a secret, common main key (11, 11'), having the following features:
- the control center (10)
 - * produces a sequence number (12) and
 - * from this and using the main key (11) produces a signing key (14) by means of one-time encryption (13), and
 - * provides the sender with the signing key (14);
 - the sender (20)
 - * uses the signing key (14) to form a signature (22c) for the message (21, 22c) and
 - * sends to the receiver a message set (22) which contains at least the message (22b) and the signature (22c).
 - The receiver (30)
 - * determines the sequence number (22a'),
 - * forms the one check key (14') using the one-time encryption (13') and the main key (11'), and
 - * uses this to check the signature (22c) on the message.
2. The method as claimed in claim 1, wherein the sequence number (12, 22a, 22a') is transmitted together with the signing key (14) from

the control center to the sender (20), and is transmitted from the sender (20) via the data set (22, 22') to the receiver.

3. The method as claimed in claim 1, wherein the
5 sequence number (12) is produced by a generator in synchronism with the number of signing and check keys used in the control center (10) and in the receiver.
4. The method as claimed in claim 1, wherein the
10 sequence number (12) is produced by a generator in synchronism with the number of signing and check keys used in the control center (10) and in the sender, and is transmitted via the data set (22, 22') to the receiver.
- 15 5. The method as claimed in one of the preceding claims, wherein the sequence number is produced by a pseudo-random number generator.
6. The method as claimed in one of the preceding
20 claims, wherein the encryption of the sequence number by means of the main key is used as the one-time encryption.
7. The method as claimed in one of the preceding
25 claims, wherein the control center (10) produces a number of signing keys (14) in advance, and transmits them to the sender (30), possibly together with the associated sequence numbers (12).
8. The method as claimed in one of the preceding
30 claims, wherein the receiver (30) maintains a list of already used sequence numbers, and rejects already used sequence numbers.

9. A device for signing a message (22, 22') which is sent from a sender (20) to a receiver (30), having the following features:

- 5 - a control center (10) and the receiver (30) have a first and a second memory for a secret, common main key (11, 11');
- 10 - in the control center (10), one input of a first one-time encrypter (13) is connected to the first protected memory (11), and another input is connected to a generator (12) for a sequence number,
- 15 - the output of the one-time encrypter (13) is connected to the sender (20) via a transport medium,
- 20 - a signature generator (24) is provided in the sender, and its inputs are connected to the output of the one-time encrypter and to the message (21, 22b) to be signed,
- 25 - the output of the signature generator (24) is connected to a device which assembles at least the signature (22c) and the message (22b) to form a message block (22) and whose output is connected to the receiver (30) via a transport medium,
- 30 - a signature checker (22') is provided in the receiver, whose inputs are connected firstly to the message (22b') and to the signature (22c) of the message block (22') which has arrived via the transport medium,
- and secondly to the output of a second one-time encrypter (13'), whose inputs are connected firstly to the second memory (11') for the

secret main key and to a means for providing a sequence number (22a').

10. The device as claimed in claim 9, wherein a generator produces the sequence number (22a') using a deterministic method, [lacuna] one or more sequence numbers corresponding to the number of checks.

Abstract

Method for signing a message, in which a control center and the receiver have a permanent, common main key. The control center produces a sequence number in advance, and a signing key from this by means of a one-time function. Both are provided in secure form to the sender. The sender uses the signing key to form a signature for the message, and sends the signature, with the sequence number and the message, to the receiver. The receiver uses a one-way function, main key and sequence number to form a check key, and thus checks the signature on the message.

Figure 1

"Version with markings to show changes made"

99P6221

- 10 -

the control center to the sender (20), and is transmitted from the sender (20) via the data set (22, 22') to the receiver.

3. The method as claimed in claim 1, wherein the
5 sequence number (12) is produced by a generator in synchronism with the number of signing and check keys used in the control center (10) and in the receiver.

4. The method as claimed in claim 1, wherein the
10 sequence number (12) is produced by a generator in synchronism with the number of signing and check keys used in the control center (10) and in the sender, and is transmitted via the data set (22, 22') to the receiver.

5. ^(Amended) The method as claimed in ^{CLAIM 1} ~~one of the preceding~~
15 ~~claims~~, wherein the sequence number is produced by a pseudo-random number generator.

6. ^(Amended) The method as claimed in ^{CLAIM 1} ~~one of the preceding~~
20 ~~claims~~, wherein the encryption of the sequence number by means of the main key is used as the one-time encryption.

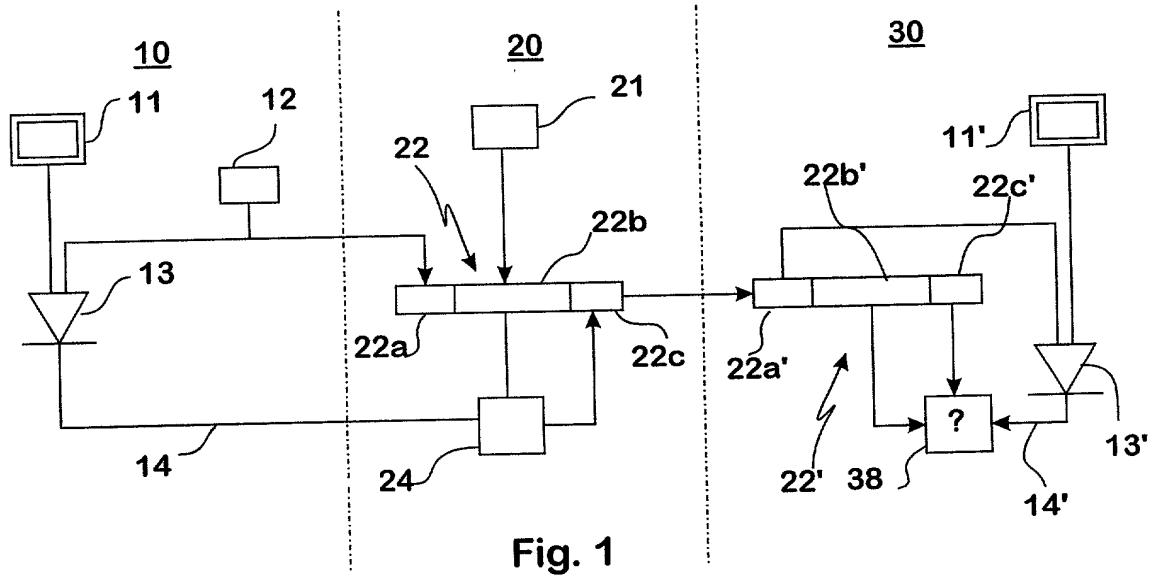
7. ^(Amended) The method as claimed in ^{CLAIM 1} ~~one of the preceding~~
25 ~~claims~~, wherein the control center (10) produces a number of signing keys (14) in advance, and transmits them to the sender (30), possibly together with the associated sequence numbers (12).

8. ^(Amended) The method as claimed in ^{CLAIM 1} ~~one of the preceding~~
30 ~~claims~~, wherein the receiver (30) maintains a list of already used sequence numbers, and rejects already used sequence numbers.

secret main key and to a means for providing a
(Amended) sequence number (22a').

10. The device as claimed in claim 9, wherein a
generator produces ~~the sequence number (22a')~~
5 using a deterministic method ~~[lacuna]~~ one or more
sequence numbers corresponding to the number of
checks.

1/1



Declaration and Power of Attorney For Patent Application

Erklärung und Vollmacht für Patentanmeldungen

German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

Signierung und Signaturprüfung von
Nachrichten

deren Beschreibung

(zutreffendes ankreuzen)

☐ hier beigefügt ist.

☒ am 07.04.2000 als

PCT internationale Anmeldung

PCT Anmeldungsnummer PCT/DE00/01086

eingereicht wurde und am

abgeändert wurde (falls tatsächlich abgeändert).

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

the specification of which

(check one)

☐ is attached hereto.

☐ was filed on _____ as

PCT international application

PCT Application No. _____

and was amended on _____

(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

German Language Declaration

Prior foreign applications
Priorität beansprucht

Priority Claimed

19919909.4	Germany	30 April 1999	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(Number)	(Country)	(Day Month Year Filed)	Yes	No
(Nummer)	(Land)	(Tag Monat Jahr eingereicht)	Ja	Nein
			<input type="checkbox"/>	<input type="checkbox"/>
(Number)	(Country)	(Day Month Year Filed)	Yes	No
(Nummer)	(Land)	(Tag Monat Jahr eingereicht)	Ja	Nein
			<input type="checkbox"/>	<input type="checkbox"/>
(Number)	(Country)	(Day Month Year Filed)	Yes	No
(Nummer)	(Land)	(Tag Monat Jahr eingereicht)	Ja	Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.)	(Filing Date)	(Status)	(Status)
(Anmeldeseriennummer)	(Anmeldedatum)	(patentiert, anhängig, aufgegeben)	(patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status)	(Status)
(Anmeldeseriennummer)	(Anmeldedatum)	(patentiert, anhängig, aufgegeben)	(patented, pending, abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: (Name und Registrationsnummer anführen)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Attorneys of the firm of McCormick, Paulding & Huber LLP as shown on the attached list

Telefongespräche bitte richten an:
(Name und Telefonnummer)

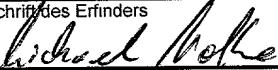
Direct Telephone Calls to: (name and telephone number)

Donald K. Huber (860) 549-5290

Postanschrift:

Send Correspondence to:

Donald K. Huber

Voller Name des einzigen oder ursprünglichen Erfinders		Full name of sole or first inventor:	
NOLTE, Michael			
Unterschrift des Erfinders	Datum	Inventor's signature	Date
	31.10.2000		
Wohnsitz		Residence	
D-33034 Brakel, Deutschland		DEX	
Staatsangehörigkeit		Citizenship	
deutsch			
Postanschrift		Post Office Address	
Koberg Weg 2a			
D-33034 Brakel			
Deutschland			
Voller Name des zweiten Miterfinders (falls zutreffend):		Full name of second joint inventor, if any:	
Unterschrift des Erfinders	Datum	Second Inventor's signature	Date
Wohnsitz		Residence	
Staatsangehörigkeit		Citizenship	
Postanschrift		Post Office Address	

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).

Voller Name des dritten Miterfinders:		Full name of third joint inventor:	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
Wohnsitz		Residence	
Staatsangehörigkeit		Citizenship	
Postanschrift		Post Office Address	
Voller Name des vierten Miterfinders (falls zutreffend):		Full name of fourth joint inventor, if any:	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
Wohnsitz		Residence	
Staatsangehörigkeit		Citizenship	
Postanschrift		Post Office Address	
Voller Name des fünften Miterfinders (falls zutreffend):		Full name of fifth joint inventor, if any:	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
Wohnsitz		Residence	
Staatsangehörigkeit		Citizenship	
Postanschrift		Post Office Address	
Voller Name des sechsten Miterfinders (falls zutreffend):		Full name of sixth joint inventor, if any:	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
Wohnsitz		Residence	
Staatsangehörigkeit		Citizenship	
Postanschrift		Post Office Address	

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).

Attachment to: German Language Declaration

McCormick, Paulding & Huber LLP
City Place II
185 Asylum Street
Hartford, Connecticut 06103-4102
U.S.A.

Telephone: (860) 549-5290
Telefax: (860) 527-0464

<u>Attorneys</u>	<u>Reg.Nos.</u>
Donald K. Huber	<u>18,686</u>
Theodore R. Paulding	<u>19,294</u>
John C. Hilton	<u>22,965</u>
Arthur F. Dionne	<u>23,093</u>
Frederick J. Haesche	<u>24,529</u>
John C. Linderman	<u>24,420</u>
J. Kevin Grogan	<u>31,961</u>
Richard R. Michaud	<u>40,088</u>
Daniel G. Mackas	<u>38,541</u>
Peter J. Rainville	<u>41,263</u>
Marina F. Cunningham	<u>38,419</u>
Susan C. Oygard	<u>42,969</u>
Nicholas J. Tuccillo	<u>44,322</u>
Stephen P. Scuderi	<u>42,136</u>
Wm. Tucker Griffith	<u>44,726</u>

15